Extra slot op 10 accounts

tijd: 15 min.

niveau: ●●○

Wil je je belangrijkste accounts écht goed beschermen, stel dan tweefactorauthenticatie in. Dat is een kleine moeite. Voor tien belangrijke accounts laten we zien hoe je dat doet.

Tekst **Rob Schleiffert / digitaalgids@consumentenbond.nl**

Voortaan log je veilig in via de DiGiD-app.

DigiD

1 Ga naar de appstore en installeer de DigiD-app.

2 Koppel de app in enkele stappen aan je DigiD-account. Hoe dat gaat, hangt af van je telefoon. Heb je een **iPhone** (waarop je geen NFC kunt gebruiken), dan zul je moeten wachten tot er een brief komt van DigiD.

3 Heb je een **Android**-toestel met NFC, dan kun je de procedure afronden. Je hebt daarvoor je gebruikersnaam en wachtwoord nodig en een identiteitsbewijs. De app vraagt je het identiteitsbewijs via de NFC-functie van je telefoon te scannen. Ook moet je een pincode van vijf cijfers bedenken (en onthouden).

4 Gelukt? Ga op de computer naar **digid.nl/inloggen** en kies inloggen via de DigiD-app.

5 Start de app en tik op **Start**. Er verschijnt een code van vier letters. Typ deze in op de site en klik op **Volgende**.

6 Scan de QR-code op het computerscherm met de app op de telefoon. Tik in de app op **Inloggen**. Tik de in Stap 2 bedachte pincode van vijf cijfers in de app. Je wordt nu op de computer ingelogd op de website van DigiD.

7 Scroll op de website naar beneden en check de inlogmethoden. Controle via sms is niet (meer) nodig en kan op 'Niet actief'. Inloggen via de app staat op 'Actief'.

8 Verbeter nog even de beveiliging. Wijzig ten slotte 'Voorkeur inlogniveau' van 'Basis' naar 'Midden'. Daarmee stel je in dat voortaan altijd de app nodig is en is je account beter beveiligd.

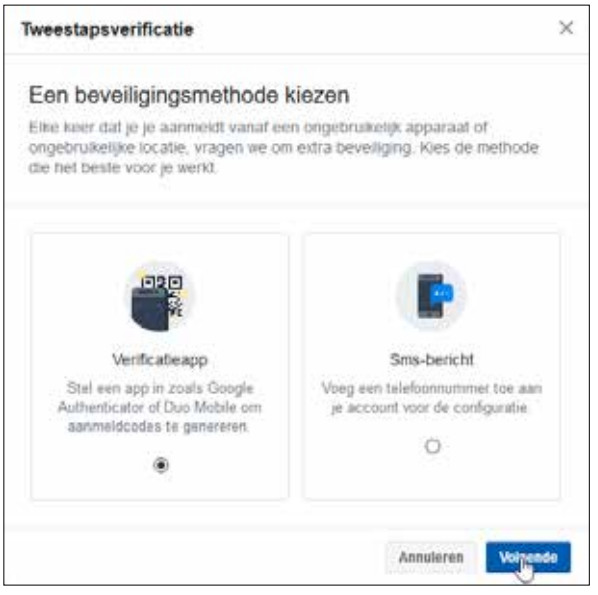
Waarom 2FA?

Je kunt nog zulke sterke wachtwoorden bedenken, als de webdienst wordt gehackt én als die de wachtwoorden niet veilig genoeg heeft opgeslagen, ligt je 'niet te kraken' wachtwoord alsnog op straat. De risico's verklein je sterk met tweefactorauthenticatie – ook wel tweestapsauthenticatie of kortweg 2FA genoemd. Het werkt heel simpel: om er zeker van te zijn dat jij degene bent die inlogt, moet je het inloggen bevestigen via een extra inlogcode of app op (doorgaans) je telefoon. Een hacker komt dus niet in je account zolang hij niet ook je telefoon heeft. Gelukkig hoef je niet iedere keer je inlog via je telefoon te bevestigen. Je kunt tijdens de eerste inlog doorgaans aangeven dat je computer vertrouwd is.

Internetbankieren

Nu bijna iedereen een smartphone heeft, vervangen de banken hun TAN-codes en inlogapparaatjes door apps. Je kunt dan een betaling via je telefoon met een vingerafdruk of pincode bevestigen. Dat is veiliger dan het gebruik van codes die per sms worden verstuurd. En het is handiger dan een e.dentifier (ABN Amro) en Rabo Scanner (Rabobank). Het installeren bij de ING gaat zo:

1 Ga naar de appstore en download de ING Mobiel Bankieren-app.
2 Pak je bankpas en beantwoord vier veiligheidsvragen.
3 Tik op **Vraag de TAN-code aan** en log op de computer in op Mijn ING. Kijk of je telefoon of tablet in de lijst staat en klik op **Activeren**.
4 Vul de TAN-code in op de website. Je krijgt er een code van zes cijfers voor terug die je invoert in de app.
5 Accepteer de voorwaarden. Bedenk (en onthoud!) een pincode. Deze kun je nodig hebben om betalingen te bevestigen.



Facebook

1 Ga naar **Instellingen** > **Beveiliging en aanmelding**.
2 Klik bij 'Tweestapsverificatie gebruiken' op **Bewerken**. Klik op **Aan de slag**.
3 Kies een van deze twee methoden: codes ontvangen per **sms-bericht** of via de **verificatie-app** van bijvoorbeeld Google of Microsoft.
4 Volg de instructies en klik op **Inschakelen**.

LET OP

Facebook krijgt hiermee je 06-nummer in handen, maar springt daar minder zorgvuldig mee om dan het beweert. Vorig jaar september bleek dat 06-nummers misbruikt werden voor het versturen van spam.

Praktijk Tweefactorauthenticatie

WhatsApp

1 Start WhatsApp > **Instellingen** > **Account** > **Verificatie in twee stappen** > **Inschakelen** (op een iPhone **Schakel in**).
2 Bedenk een willekeurige, maar wel te onthouden pincode van zes cijfers en vul die in.
3 Vul jemailadres in. Als je de pincode toch vergeet, kun je de code via de mail resetten.
4 WhatsApp zal je geregeld om de code vragen. Ook als je je wilt aanmelden via een andere telefoon zul je de code moeten invullen.

WhatsApp vraagt geregeld om je pincode.

PayPal

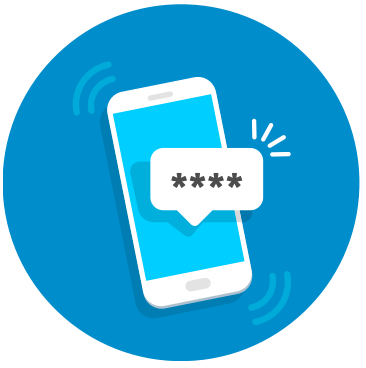
1 Log in op paypal.com en ga naar **Instellingen** > **Veiligheid**. Klik naast 'Tweestapsverificatie' op **Instellen**.
2 Kies een methode: een **sms-bericht** ontvangen of een **verificatie-app** gebruiken. Klik op **Volgende**.
3 Volg de aanwijzingen en kies een back-upmethode voor het geval je je telefoon verliest.
4 Klik op Klaar.

LinkedIn

1 Log in op **linkedin.com** en klik op je profielpictogram > **Instellingen en privacy**.
2 Klik op tabblad **Account** en klik bij 'Dubbele verificatie' op **Wijzigen**.
3 Klik op **Inschakelen**. Als LinkedIn je mobielnummer al kent, krijg je meteen een controlecode toegestuurd.
4 Vul de code van zes cijfers in op de website. Klik op **Verifiëren**.

Twitter

1 Ga naar **twitter.com** en log in.
2 Klik aan de linkerkant op het icoon met de drie puntjes > **Instellingen en privacy** > **Account**.
3 Klik op **Beveiliging** > **Inlogverificatie**. Schakel de functie in.
4 Geef nogmaals je wachtwoord in en bevestig je telefoonnummer. Twitter stuurt nu een sms.
5 Vul de code (zes cijfers) in op de site. Klik op **Back-upcode ontvangen** voor het geval je je telefoon verliest. Kopieer de code en bewaar hem goed.
6 Kies een methode: een code per **sms** of via een **veiligheidsapp**, bijvoorbeeld van Google of Microsoft (zie onder Google en Microsoft).



SMS of verificatieapp?

Veel 2FA gaat nog steeds via sms'jes. Je ontvangt een tekstberichtje met een code die je op de site moet invullen. Sms-verkeer is een overblijfsel uit een ver verleden en niet meer helemaal veilig: in theorie kunnen hackers zulke berichtjes onderscheppen.
Een snellere en veilige methode is het gebruik van een verificatieapp. Zo'n gratis app voor je telefoon koppel je aan een account (mailadres) en genereert iedere 30 seconden een code van zes cijfers. Die is versleuteld en niet te onderscheppen. De bekendste zijn de Authenticator-apps van Google en Microsoft.
Een derde methode is het gebruik van een (usb-)stick als authenticatiesleutel.

Google / Gmail

1 Ga naar **google.com/landing/2step** en klik op **Aan de slag** en log in op je Google-account.
2 Klik op **Aan de slag**. Weet Google je 06-nummer nog niet, dan vul je dat nu in.
3 Je ontvangt meteen een controlebericht op je telefoon. Bevestig de ontvangst.
4 Kies op de computer de manier waarop je de codes wilt ontvangen: per sms of telefoonoproep. Kies **Sms** > **Verzenden**. Je ontvangt nu een code op je telefoon. Vul die in op de computer. Authenticatie in twee stappen is nu ingeschakeld.
5 Kies nu alternatieve controlemanieren. Download een lijst met tien back-upcodes voor het geval je de telefoon kwijtraakt. En kies ervoor om de controlecodes in de Google Authenticator-app te ontvangen. Dat is veiliger dan per sms. Klik op **Instellen** en kies je type telefoon.
7 Download nu de app uit de appstore op je smartphone en volg de stappen. Voeg je account toe door met de app de blokjescode (QR-code) op het computerscherm te scannen. Vul de zescijferige code die de telefoon opgeeft, in op de computer en klik op **Verifiëren**.
8 Vanaf nu zal Google je een blokjescode laten zien zodra je via een andere computer bij Google inlogt. Scan die code met de app. Dat hoeft maar één keer als je een vinkje zet bij de regel dat je vaker van dit apparaat gebruikmaakt.

Microsoft / Outlook.com

1 Log in op **login.live.com/nl**.
2 Klik op **Beveiliging** > **Meer beveiligingsopties**.
3 Kies **Verificatie in twee stappen instellen**. Klik op **Volgende**.
4 Je kunt nu kiezen: verificatie via een app, telefoonnummer (sms of spraakoproep) of een ander e-mailadres. Kies je voor de app, dan moet je op je smartphone de **Microsoft Authenticator** installeren. Open de app en volg de korte aanmeldinstructies.
5 Klik op de computer op **Volgende** om de verificatie in te schakelen. Je krijgt nu een herstelcode van 25 letters en cijfers voor het geval je niet meer op een andere manier kunt inloggen. Klik op **Volgende** om af te ronden.
6 De app gebruik je alleen als je je via een 'niet vertrouwd' apparaat wilt aanmelden bij een Microsoft-dienst. Dat is een computer of smartphone waarmee je nog niet eerder hebt ingelogd. Zodra je inlogt, stuurt Microsoft je via de app een berichtje ter controle.

Apple

In iOS:
1 In iOS: ga naar **Instellingen** > [je naam] > **Wachtwoord en beveiliging**
2 Tik bij **Twee-factor-authenticatie** op **Aan**.
3 Tik op **Ga door**.

In MacOS:
1 Ga naar het Apple-menu > **Systeemvoorkeuren** > **iCloud** > **Accountgegevens**.
2 Klik op **Beveiliging**.
3 Klik op **Zet twee-factor-authenticatie aan**.

Consumenten bond

Hoe herken je digitale zakkenrollers?

In de Digitaalgids vind je praktische tips en adviezen.
consumentenbond.nl/digitaalgids